Notice of Allowability	Application No.	Applicant(s)	
	09/741,691	SAMAR, VIPIN	
	Examiner	Art Unit	
	Linh LD Son	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *11/09/06*.

2. ☒ The allowed claim(s) is/are *1,7-12,18-23 and 29-33*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *12/13/06* .
7. ☒ Examiner's Amendment/Comment
8. ☐ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

DETAILED ACTION

Response to Arguments

1. Applicant's arguments, see After Final, filed 11/09/06, with respect to claims 1, 7-12, 18-23, and 29-33 have been fully considered and are persuasive. The Rejection dated 09/22/06 of claims 1, 7-12, 18-23, and 29-33 has been withdrawn.

EXAMINER'S AMENDMENT

2. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Attorney Ed Grundler on 12/13/06.

The application has been amended as follows:

1. (Currently amended) A method for facilitating the delegation of operations involved in providing digital signatures to a signature server, the method comprising:

allowing a user to authenticate the signature server prior to sending a message to the signature server;

receiving the message from the user at the signature server, the message including an item to be signed on behalf of the user by the signature server, a user identifier which identifies the user, and an application identifier which identifies the application being used;

authenticating the user at the signature server;

determining whether the user is authorized to request a signature for ~~sign~~ the item by communicating with an authority server that is separate from the signature server, wherein determining whether the user is authorized to request a signature for the item involves looking up an authorization for the user based upon an identifier for the user as well as an identifier for an application to which the user will send the signed item after it has been signed and returned by the signature server;

looking up a private key for the user at the signature server based on the user identifier and the application identifier, wherein looking up a private key for the user based on the user identifier and application identifier, and wherein using the private key prevents a user who is allowed to access a second application, but who is not allowed to access the application being used, from gaining access to the application being used; and

if the private key is found, signing the item with the private key for the user.

2-6 (Canceled).

7. (Previously presented) The method of claim 1, further comprising returning the signed item to the user so that the user can send the signed item to a recipient.

8. (Original) The method of claim 1, wherein the method further comprises configuring the signature server to accommodate a new user by:

receiving a request from an authorized entity to add the new user;

generating a key pair for the new user, including a new user private key and a new user public key;

communicating with a certification authority to obtain a certificate for the new user based on the key pair; and

storing the certificate and the key pair for the new user in a location that is accessible by the signature server to enable the signature server to sign items on behalf of the new user.

9. (Original) The method of claim 1, wherein the method further comprises configuring the signature server to delete an old user by:

receiving a request from an authorized entity to delete the old user;

notifying a certification authority to revoke a certificate for the old user; and

removing the private key for the old user from the signature server, so that the signature server can no longer sign items on behalf of the old user.

10. (Previously presented) The method of claim 1, wherein the method further comprises archiving the message and the signed item at the signature server.

11. (Original) The method of claim 1, wherein the method further comprises forwarding the signed item to an archive server in order to be archived.

12. (Currently amended) A computer-readable storage medium storing instructions that when executed by a computer cause the computer to perform a method for facilitating the delegation of operations involved in providing digital signatures to a signature server, wherein the computer-readable storage medium is selected from a group consisting of magnetic and optical storage devices, disk drives, magnetic tape, CDs (compact discs), and DVDs (digital versatile discs or digital video discs), the method comprising:

allowing a user to authenticate the signature server prior to sending a message to the signature server;

receiving the message from the user at the signature server, the message including an item to be signed on behalf of the user by the signature server, a user identifier which identifies the user, and an application identifier which identifies the application being used;

authenticating the user at the signature server;

determining whether the user is authorized to request a signature for ~~sign~~ the item by communicating with an authority server that is separate from the signature

server, wherein determining whether the user is authorized to request a signature for the item involves looking up an authorization for the user based upon an identifier for the user as well as an identifier for an application to which the user will send the signed item after it has been signed and returned by the signature server;

looking up a private key for the user at the signature server based on the user identifier and the application identifier, wherein looking up a private key for the user based on the user identifier and application identifier, and wherein using the private key prevents a user who is allowed to access a second application, but who is not allowed to access the application being used, from gaining access to the application being used; and

if the private key is found, signing the item with the private key for the user.

13-17 (Canceled).

18. (Previously presented) The computer-readable storage medium of claim 12, wherein the method further comprises returning the signed item to the user so that the user can send the signed item to a recipient.

19. (Original) The computer-readable storage medium of claim 12, wherein the method further comprises configuring the signature server to accommodate a new user by:

receiving a request from an authorized entity to add the new user;

generating a key pair for the new user, including a new user private key and a new user public key;

communicating with a certification authority to obtain a certificate for the new user based on the key pair; and

storing the certificate and the key pair for the new user in a location that is accessible by the signature server to enable the signature server to sign items on behalf of the new user.

20. (Original) The computer-readable storage medium of claim 12, wherein the method further comprises configuring the signature server to delete an old user by:

receiving a request from an authorized entity to delete the old user;

notifying a certification authority to revoke a certificate for the old user; and

removing the private key for the old user from the signature server, so that the signature server can no longer sign items on behalf of the old user.

21. (Previously presented) The computer-readable storage medium of claim 12, wherein the method further comprises archiving the message and the signed item at the signature server.

22. (Original) The computer-readable storage medium of claim 12, wherein the method further comprises forwarding the signed item to an archive server in order to be archived.

23. (Currently amended) An apparatus that facilitates delegating operations involved in providing digital signatures, comprising:

a signature server;

an authentication mechanism that is configured to allow a user to authenticate the signature server prior to sending a message to the signature server

a receiving mechanism within the signature server that is configured to receive the message from the user, the message including an item to be signed on behalf of the user by the signature server, a user identifier which identifies the user, and an application identifier which identifies the application being used;

an authenticating mechanism configured to authenticate the user at the signature server;

a determining mechanism configured to determine whether the user is authorized request a signature for ~~sign~~ the item by communicating with an authority server that is separate from the signature server, wherein determining whether the user is authorized to request a signature for the item involves looking up an authorization for the user based upon an identifier for the user as well as an identifier for an application to which the user will send the signed item after it has been signed and returned by the signature server;

a lookup mechanism within the signature server that is configured to look up a private key for the user based on the user identifier and the application identifier, wherein looking up a private key for the user based on the user identifier and application

identifier, and wherein using the private key prevents a user who is allowed to access a second application, but who is not allowed to access the application being used, from gaining access to the application being used; and

a signing mechanism within the signature server that is configured to sign the item with the private key for the user if the private key is found.

24-28 (Canceled).

29. (Previously presented) The apparatus of claim 23, further comprising a sending mechanism within the signature server that is configured to return the signed item to the user so that the user can send the signed item to a recipient. 30. (Original) The apparatus of claim 23, further comprising an initialization mechanism that is configured to:

receive a request from an authorized entity to add a new user;

generate a key pair for the new user, including a new user private key and a new user public key;

communicate with a certification authority to obtain a certificate for the new user based on the key pair; and to

store the certificate and the key pair for the new user in a location that is accessible by the signature server to enable the signature server to sign items on behalf of the new user.

31. (Original) The apparatus of claim 23, further comprising a deletion mechanism that is configured to:

receive a request from an authorized entity to delete an old user;

notify a certification authority to revoke a certificate for the old user; and to

remove the private key for the old user from the signature server, so that the signature server can no longer sign items on behalf of the old user.

32. (Previously presented) The apparatus of claim 23, further comprising an archiving mechanism that is configured to archive the message and the signed item at the signature server.

33. (Original) The apparatus of claim 23, further comprising an archiving mechanism that is configured to forward the signed item to an archive server in order to be archived.

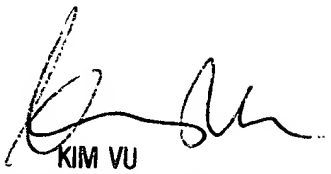
3. Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Linh LD Son whose telephone number is 571-272-3856. The examiner can normally be reached on 9-6 (M-F).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Linh LD Son
Examiner
Art Unit 2135



KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

***